Project Update: A New Foundation of Attack Trees in Linear Logic

Harley Eades III

Computer Science
Augusta University
harley.eades@gmail.com

Abstract. In this short paper I provide an update on the status of newly funded research project investigating founding attack trees in the resource conscious theory called linear logic. I introduce a new linear logic called the Attack Tree Linear Logic (ATLL) which models attack trees as formulas and uses implication to reason about attack trees. I then introduce a new generalization of Bucciarelli and Ehrhards indexed linear logic to obtain Indexed ATLL which adds costs to attack trees. The most interesting aspect of Indexed ATLL is that implication is endowed with a relation for taking into consideration the costs while reasoning about attack trees.

1 Introduction

What is a mathematical model of attack trees? There have been numerous proposed answers to this question. Some examples are propositional logic, multisets, directed acyclic graphs, source sink graphs (or parallel-series pomsets), Petri nets, and Markov processes. Is there a unifying foundation in common to each of these proposed models? Furthermore, can this unifying foundation be used to further the field of attack trees and build new tools for conducting threat analysis?

The answer to the first question is positive, but the answer to the second question is open. Each of the proposed models listed above have something in common. They can all be modeled in some form of a symmetric monoidal category [6,1,2,3]. That is all well and good, but what can we gain from monoidal categories?

Monoidal categories are a mathematical model of linear logic as observed through the beautiful Curry-Howard-Lambek correspondence [5]. In linear logic every hypothesis must be used exactly once, and hence, if we view a hypothesis as a resource, then this property can be stated as every resource must be consumed. This linearity property is achieved by removing the structural rules for weakening and contraction from classical or intuitionistic logic. Thus, from a resource perspective, resources cannot be spontaneously created or duplicated – hence, propositional logic can be viewed as a degenerate, from a resource perspective, form of linear logic.

Multisets and Petri nets both capture the idea that the nodes of an attack tree capture both the attack action and the state – the resource – of the system being analyzed. As it turns out, linear logic has been shown to be a logical foundation for multisets [6] and Petri Nets [1]. Thus, linear logic has the ability to model the state as well as attack actions of the goals of an attack tree. I propose that linear logic be used as the logical foundation of attack trees.

This projects[1] main goal is to determine the suitability of linear logic as a foundation for attack trees. In this short paper I give an update on this project and introduce a new logical foundation of attack trees. The type of attack trees considered in this paper are attack trees with sequential composition similar to Jhawar et al. [4]. Attack trees consist of two layers: the logical layer or process tree, and the quantitative layer. One interesting aspect of my proposed foundation is that both layers can be considered during reasoning about attack trees.

At the logical layer the base attacks of an attack tree will correspond to atomic formulas in linear logic, and each branching node of an attack tree will correspond to a binary operator in linear logic. Adding costs corresponds to annotating the atomic formulas with some base cost, and then annotating the binary operators with a cost computed from the costs of their respective left operand (left subtree) and right operand (right subtree). The most interesting aspect of adding costs is that computing the costs at the branching nodes is done during the construction of a derivation using the inference rules of the logic.

The inference rules of linear logic provide a number of benefits when constructing attack trees. First, the inference rules will certify that an attack tree is constructed correctly and all costs on branching nodes will be computed from the costs of the left and right subtrees. On top of that the inference rules offer a means of proving when two attack trees are equivalent. Leveraging the fact that language of attack trees corresponds to a very simple fragment of linear logic, e.g. linear implication is not needed, I conjecture that proving equivalence of attack trees can be automated. Thus, this could be used in practice to certify the correctness of transformations of attack trees maintaining the resource based semantics.

2 Attack Trees without Costs

In this section I introduce attack trees with sequential composition – sometimes referred to SAND attack trees – without cost annotations in the hope that doing so will make the main ideas of this work more clear to the reader. This formulation of attack trees was first proposed by Jhawar et al. [4]. First, I define the syntax of attack trees then a linear logic for reasoning about attack trees.

[1] This material is based upon work supported by the National Science Foundation CRII CISE Research Initiation grant, "CRII:SHF: A New Foundation for Attack Trees Based on Monoidal Categories", under Grant No. 1565557.

Definition 1. *Suppose* B *is a set of base attacks whose elements are denoted by* b*. Then an* ***attack tree*** *is defined by the following grammar:*

$$T ::= b \mid T_1 \odot T_2 \mid T_1 \sqcup T_2 \mid T_1 \rhd T_2$$

I denote unsynchronized parallel composition of attacks by $T_1 \odot T_2$*, choice between attacks by* $T_1 \sqcup T_2$*, and sequential composition of attacks by* $T_1 \rhd T_2$*.*

Now we define the attack tree linear logic (ATLL) for reasoning about attack trees. In ATLL attack trees are modeled as formulas, and thus, if attack trees are formulas, then reasoning about attack trees should correspond to proving implications between attack trees. Furthermore, some care must be taken so that choice and parallel composition are symmetric, but sequential composition is not. We enforce this property in ATLL by separating hypotheses as is usually done in ordered linear logic [**?**].

Definition 2. *Suppose* B *is a set of base attacks whose elements are denoted by* b*. The syntax of ATLL formulas and contexts are defined as follows:*

$$\begin{aligned} \textit{(formulas)}\ E &::= b \mid E_1 \odot E_1 \mid E_1 \sqcup E_2 \mid E_1 \rhd E_2 \mid E_1 \multimap E_2 \\ \textit{(base contexts)}\ \Gamma, \Delta &::= \cdot \mid b \mid \Gamma, \Delta \\ \textit{(general contexts)}\ \Theta, \Psi &::= \cdot \mid E \mid \Gamma, \Delta \end{aligned}$$

$$\frac{}{\cdot; b \vdash^T b}\ \mathrm{id}_{\odot} \qquad \frac{}{b; \cdot \vdash^T b}\ \mathrm{id}_{\rhd} \qquad \frac{\Gamma_1; \Delta_1 \vdash^T T_1 \quad \Gamma_2; \Delta_2 \vdash^T T_2}{\Gamma_1, \Gamma_2; \Delta_1, \Delta_2 \vdash^T T_1 \odot T_2}\ \odot$$

$$\frac{\Gamma_1; \Delta_1 \vdash^T T_1 \quad \Gamma_2; \Delta_2 \vdash^T T_2}{\Gamma_1, \Gamma_2; \Delta_1, \Delta_2 \vdash^T T_1 \rhd T_2}\ \rhd \qquad \frac{\Gamma_1; \Delta_1 \vdash^T T_1 \quad \Gamma_2; \Delta_2 \vdash^T T_2}{\Gamma_1, \Gamma_2; \Delta_1, \Delta_2 \vdash^T T_1 \sqcup T_2}\ \sqcup$$

Fig. 1. Well Formed Attack Trees in ATLL

ATLL formulas are defined as an extension of the syntax for attack trees with linear implication. An attack tree then corresponds to an ATLL formula without implication. Suppose E is an ATLL formula such that every base attack in E which is a leaf of sequential composition is in the base context Γ, and every leaf of parallel composition is in the base context Δ. Then E is an attack tree if and only if $\Gamma; \Delta \vdash^T E$ holds with respect to the rules in Figure 1.

The inference rules in Figure 1 enforce several properties. First, they enforce that every base attack is used exactly once, and that an attack tree does not mention linear implication. Furthermore, they allow us to restrict our reasoning to attack trees which I conjecture will result in our reasoning being more amenable to automation.

$$\frac{}{\cdot; E \vdash E}\,\mathrm{id}_{\odot} \qquad \frac{}{E; \cdot \vdash E}\,\mathrm{id}_{\triangleright} \qquad \frac{\Theta_1; \Psi_1 \vdash E_1 \quad \Theta_2; \Psi_2 \vdash E_2}{\Theta_1, \Theta_2; \Psi_1, \Psi_2 \vdash E_1 \odot E_2}\,\odot_I$$

$$\frac{\Theta_1; \Psi_2 \vdash E_1 \odot E_2 \quad \Theta_2; \Psi_1, E_1, E_2, \Psi_3 \vdash E_3}{\Theta_1, \Theta_2; \Psi_1, \Psi_2, \Psi_3 \vdash E_3}\,\odot_E \qquad \frac{\Theta_1; \Psi_1 \vdash E_1 \quad \Theta_2; \Psi_2 \vdash E_2}{\Theta_1, \Theta_2; \Psi_1, \Psi_2 \vdash E_1 \rhd E_2}\,\rhd_I$$

$$\frac{\Theta_2; \Psi_2 \vdash E_1 \rhd E_2 \quad \Theta_1, E_1, E_2, \Theta_3; \Psi_2 \vdash E_3}{\Theta_1, \Theta_2, \Theta_3; \Psi_1, \Psi_2 \vdash E_3}\,\rhd_E \qquad \frac{\Theta; \Psi_1, E_1, E_2, \Psi_2 \vdash E}{\Theta; \Psi_1, E_2, E_1, \Psi_2 \vdash E}\,\mathrm{sym}_{\odot}$$

$$\frac{\Theta_1; \Psi_1 \vdash E_1 \quad \Theta_2; \Psi_2 \vdash E_2}{\Theta_1, \Theta_2; \Psi_1, \Psi_2 \vdash E_1 \sqcup E_2}\,\sqcup \qquad \frac{\Theta; \Psi, E_1 \vdash E_2}{\Theta; \Psi \vdash E_1 \multimap E_2}\,\multimap_I$$

$$\frac{\Theta_1; \Psi_1 \vdash E_1 \multimap E_2 \quad \Theta_2; \Psi_2 \vdash E_1}{\Theta_1, \Theta_2; \Psi_1, \Psi_2 \vdash E_2}\,\multimap_E$$

Fig. 2. ATLL Logical Inference Rules

$$\frac{\Theta; \Psi \vdash T}{\Theta; \Psi \vdash (T \sqcup T) \circ\!\!\multimap T}\,\mathrm{cont}_{\sqcup} \qquad \frac{\Theta; \Psi \vdash T_1 \sqcup T_2}{\Theta; \Psi \vdash (T_1 \sqcup T_2) \circ\!\!\multimap (T_2 \sqcup T_1)}\,\mathrm{sym}_{\sqcup}$$

$$\frac{\Theta; \Psi \vdash (T_1 \sqcup T_2) \sqcup T_3}{\Theta; \Psi \vdash ((T_1 \sqcup T_2) \sqcup T_3) \circ\!\!\multimap (T_1 \sqcup (T_2 \sqcup T_3))}\,\mathrm{assoc}_{\sqcup}$$

$$\frac{\Theta; \Psi \vdash^{T} T_1 \odot (T_2 \rhd T_3)}{\Theta; \Psi \vdash (T_1 \odot (T_2 \sqcup T_3)) \circ\!\!\multimap ((T_1 \odot T_2) \sqcup (T_1 \odot T_3))}\,\mathrm{dis}_{\odot}$$

$$\frac{\Theta; \Psi \vdash^{T} T_1 \rhd (T_2 \sqcup T_3)}{\Theta; \Psi \vdash (T_1 \rhd (T_2 \sqcup T_3)) \circ\!\!\multimap ((T_1 \rhd T_2) \sqcup (T_1 \rhd T_3))}\,\mathrm{dis}_{\rhd}$$

Fig. 3. ATLL Attack Tree Axioms

The ATLL logical inference rules are defined in Figure 2. These rules make up a basic linear logic for attack trees. For example, we can prove that sequential and parallel composition are associative, and the latter is symmetric, but there are a number of facts that these rules do not prove. They cannot prove that choice is associative and symmetric, and they cannot prove the usual distributive laws associated with attack trees with sequential composition [4]. To overcome this limitation we add the attack tree axioms in Figure 3 to ATLL. The logical connective $\multimap\!\!\circ$ is linear biimplication which is defined in the usual way as classical implication. The reader should note that these axioms are restricted to attack trees only and not applicable to full ATLL formulas.

The ATLL logical inference rules also make it clear why we separate hypotheses into two contexts. The exchange rule, $\mathrm{sym}_{\odot}$, allows one to exchange hypotheses in the context Ψ, but notice that there is no exchange rule for the context Θ. Thus, one should think of the hypotheses in Ψ as running in parallel and the hypotheses in Θ as running sequentially. In fact, this interpretation is reinforced by the elimination rules, $\odot_E$ and $\rhd_E$, for parallel and sequential conjunction respectively.

Finally, ATLL allows one to prove every equivalence for attack trees with sequential composition given by Jhawar et al. [4] as linear implications. I conjecture that it should be possible to define a proof search algorithm for ATLL to automate equational reasoning on attack trees, but this is future work. However, using implication as a means to reason about attack trees opens the door for different types of reasoning.

Suppose T_1 is a larger attack tree, and we wish to know if the attack tree T_2 is contained within T_1, that is, T_2 is a subattack tree of T_1. Currently, ATLL will not allow us to prove this, but it can if we add the following rules:

$$\frac{\Theta_1, \Theta_2; \Psi \vdash E \quad \Gamma; \Delta \vdash^T T}{\Theta_1, T, \Theta_2; \Psi \vdash E}\ \mathrm{wk}_{\odot} \qquad \frac{\Theta; \Psi_1, \Psi_2 \vdash E \quad \Gamma; \Delta \vdash^T T}{\Theta; \Psi_1, T, \Psi_2 \vdash E}\ \mathrm{wk}_{\rhd}$$

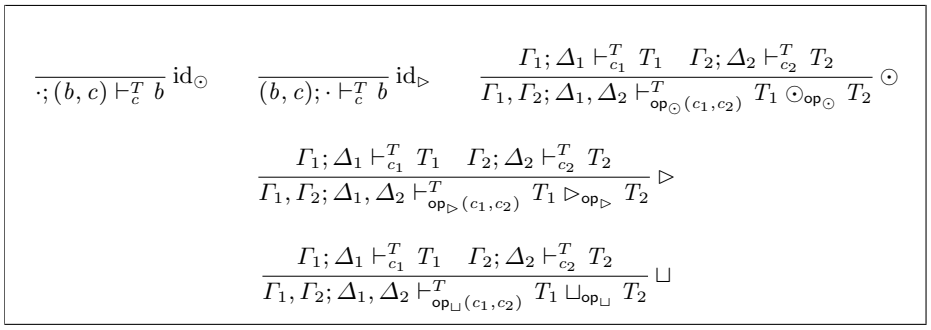
These rules allow us to discard parts of a larger attack tree while constructing proof derivations, but this only works for attack trees not general ATLL formulas. Thus, with these rules ATLL becomes slightly affine. We can now use these rules to determine if $T_1 \multimap T_2$ holds, and if it does, then T_2 is a subattack tree of T_1.

3 Attack Trees with Costs

By generalizing Bucciarelli and Ehrhards indexed linear logic [**?**] one obtains a means of adding costs to attack trees. In addition, I extend ATLL into Indexed ATLL with the ability to reason about the costs while reasoning about attack trees.

Definition 3. *Suppose* B *is a set of base attacks whose elements are denoted by* b*, and* C *is a set of costs whose elements are denoted by* c*. Additionally, let* $(\mathsf{C}, \mathsf{op}_{\odot})$ *and* $(\mathsf{C}, \mathsf{op}_{\sqcup})$ *be symmetric monoids on* C*, and* $(\mathsf{C}, \mathsf{op}_{\rhd})$ *be a monoid on* C*. Then an* ***attack tree with costs*** *is defined by the following grammar:*

$$T ::= (b, c) \mid T_1 \odot_{\mathsf{op}_{\odot}} T_2 \mid T_1 \sqcup_{\mathsf{op}_{\sqcup}} T_2 \mid T_1 \rhd_{\mathsf{op}_{\rhd}} T_2$$



$$\frac{}{\cdot;(b,c) \vdash^T_c b}\ \mathrm{id}_{\odot} \qquad \frac{}{(b,c);\cdot \vdash^T_c b}\ \mathrm{id}_{\triangleright} \qquad \frac{\Gamma_1;\Delta_1 \vdash^T_{c_1} T_1 \quad \Gamma_2;\Delta_2 \vdash^T_{c_2} T_2}{\Gamma_1,\Gamma_2;\Delta_1,\Delta_2 \vdash^T_{\mathsf{op}_{\odot}(c_1,c_2)} T_1 \odot_{\mathsf{op}_{\odot}} T_2}\ \odot$$

$$\frac{\Gamma_1;\Delta_1 \vdash^T_{c_1} T_1 \quad \Gamma_2;\Delta_2 \vdash^T_{c_2} T_2}{\Gamma_1,\Gamma_2;\Delta_1,\Delta_2 \vdash^T_{\mathsf{op}_{\triangleright}(c_1,c_2)} T_1 \triangleright_{\mathsf{op}_{\triangleright}} T_2}\ \triangleright$$

$$\frac{\Gamma_1;\Delta_1 \vdash^T_{c_1} T_1 \quad \Gamma_2;\Delta_2 \vdash^T_{c_2} T_2}{\Gamma_1,\Gamma_2;\Delta_1,\Delta_2 \vdash^T_{\mathsf{op}_{\sqcup}(c_1,c_2)} T_1 \sqcup_{\mathsf{op}_{\sqcup}} T_2}\ \sqcup$$

Fig. 4. Well Formed Attack Trees in Indexed ATLL

Each base attack is annotated with a cost, and every branching node is annotated with a binary operation for computing the cost at that node using the costs of the left subtree and the right subtree.

I now extend the syntax and rules of ATLL into Indexed ATLL, but due to space I do not give every rule here, but only the most interesting ones, because they are similar to ATLL; the entire system is defined in Appendix **??**.

Definition 4. *Suppose* B *is a set of base attacks whose elements are denoted by* b*, and* C *is a set of costs whose elements are denoted by* c*. Additionally, let* $(\mathsf{C}, \mathsf{op}_{\odot})$ *and* $(\mathsf{C}, \mathsf{op}_{\sqcup})$ *be symmetric monoids on* C*, and* $(\mathsf{C}, \mathsf{op}_{\triangleright})$ *be a monoid on* C*. Furthermore, let* $(\mathsf{C}, \mathsf{rel}_{\multimap})$ *be a preorder on* C*. Then the syntax of Indexed ATLL formulas and contexts are defined as follows:*

$$\begin{aligned} \textit{(formulas)}\ E &::= (b,c) \mid E_1 \odot_{\mathsf{op}_{\odot}} E_1 \mid E_1 \sqcup_{\mathsf{op}_{\sqcup}} E_2 \mid E_1 \triangleright_{\mathsf{op}_{\triangleright}} E_2 \\ &\quad \mid E_1 \multimap_{\mathsf{rel}_{\multimap}(c,-)} E_2 \\ \textit{(base contexts)}\ \Gamma,\Delta &::= \cdot \mid (b,c) \mid \Gamma,\Delta \\ \textit{(general contexts)}\ \Theta,\Psi &::= \cdot \mid (E,c) \mid \Gamma,\Delta \end{aligned}$$

The most interesting addition here is implication denoted $E_1 \multimap_{\mathsf{rel}_{\multimap}(c,-)} E_2$. The cost, c, is the cost of the formula E_1, and then the unary relation $\mathsf{rel}_{\multimap}(c,-)$ will be used to determine if the cost of E_1 is related to the cost of E_2 when proving an implication between E_1 and E_2.

The inference rules for well-formed attack trees in Indexed ATLL are given in Figure 4. The judgment is now denoted by $\Gamma;\Delta \vdash^T_c T$ where c is the fully computed cost of the root of the attack tree T. Notice that this cost is computed during the construction of a proof derivation. This cost will be used along with the relation on implication to influence the relationship between attack trees.

The logical inference rules for Indexed ATLL are given in Figure 5. As I mentioned above I only give a select few of the rules here, but the complete system can be found in Appendix **??**. The most interesting rule is the introduction rule for implication, $\multimap_I$, because the second premise is $\mathsf{rel}_{\multimap}(c_1, c_2)$.

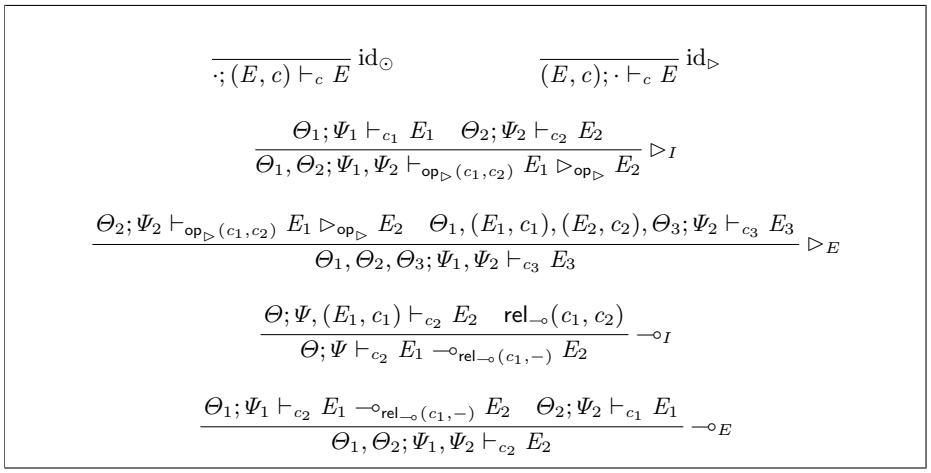


Fig. 5. Select Logical Inference Rules for Indexed ATLL

Suppose (T_1, c_1) and (T_2, c_2) are two attack trees with the respective costs, and the relation $\mathsf{rel}_{\multimap}(c_1, c_2)$ holds if and only if $c_1 \leq c_2$. If we wanted to show that the attack tree T_1 is equivalent to the attack tree T_2, then we would have to show $T_1 \circ\!\!-\!\!\circ_{\mathsf{rel}_{\circ\multimap}(c_1,-)} T_2$ where $\mathsf{rel}_{\circ\multimap}(c_1, c_2)$ if and only if $\mathsf{rel}_{\multimap}(c_1, c_2)$ and $\mathsf{rel}_{\multimap}(c_2, c_1)$. This would require one to prove $\mathsf{rel}_{\circ\multimap}(c_1, c_2)$ which would require $c_1 = c_2$. Thus, in this example, attack trees would be equivalent if and only if they have the same logical structure and the same overall cost. Thus, several different types of reasoning on attack trees can be modeled in Index ATLL depending on the relation chosen for implication.

4 Conclusion and Future Work

I introduced a new linear logic for reasoning about attack trees called the Attack Tree Linear Logic (ATLL) with and without costs. Attack trees are modeled as logical formulas and proving relationships between attack trees corresponds to proving implications. Adding costs to ATLL results in a new indexed linear logic called Indexed ATLL. Then I showed how endowing implication with a relation on costs can be used include the costs when reasoning about attack trees.

ATLL is just one part of this project, the following are some next steps with respect to (Indexed) ATLL and other parts of the project:

- Define a term assignment for (Indexed) ATLL that can be used to define attack trees using a functional programming language.
- Determine the applicability of automating reasoning on attack trees in (Indexed) ATLL using proof search.
- Finish studying the categorical model to which (Indexed) ATLL is based.

– Finishing the development of a modular and stand alone IDE for attack tree in Javascript that can be used with various formalization of attack trees. Hopefully, that the community will be able to make use of this interface.

References

1. Carolyn Brown, Doug Gurr, and Valeria Paiva. A linear specification language for petri nets. *DAIMI Report Series*, 20(363), 1991.
2. Marcelo Fiore and Marco Devesas Campos. *Computation, Logic, Games, and Quantum Foundations. The Many Facets of Samson Abramsky: Essays Dedicated to Samson Abramsky on the Occasion of His 60th Birthday*, chapter The Algebra of Directed Acyclic Graphs, pages 37–51. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
3. Luisa Francesco Albasini, Nicoletta Sabadini, and Robert F. C. Walters. The compositional construction of markov processes. *Applied Categorical Structures*, 19(1):425–437, 2010.
4. Ravi Jhawar, Barbara Kordy, Sjouke Mauw, SaÅ!'a RadomiroviÄ, and Rolando Trujillo-Rasua. Attack trees with sequential conjunction. In Hannes Federrath and Dieter Gollmann, editors, *ICT Systems Security and Privacy Protection*, volume 455 of *IFIP Advances in Information and Communication Technology*, pages 339–353. Springer International Publishing, 2015.
5. Paul-André Melliès. Categorical semantics of linear logic. In Pierre-Louis Curien, Hugo Herbelin, Jean-Louis Krivine, and Paul-André Melliès, editors, *Interactive models of computation and program behaviour*. Panoramas et Synthèses 27, Société Mathématique de France, 2009.
6. A Tzouvaras. The linear logic of multisets. *Logic Journal of IGPL*, 6(6):901–916, 1998.

Appendix